quiz 10.1

(1) Find four different square roots of 9 modulo 3379. Specifically, find two more in addition to the 'obvious' square roots ± 3.

(2) The integer 140873 is known to be a product of two distinct primes. You have access to a square-root oracle which can take square roots of squares modulo 140873. When you give the oracle $7 \cdot 7$ to take the square root, it returns 65328. Factor 140873.

(3) Consider the quadratic polynomial x^2-5x+6 as having coefficients in $\mathbf{Z}/299$. In addition to the 'obvious' factorization $x^2 - 5x + 6 = (x - 2) \cdot (x - 3)$ find another completely different factorization.

(4) Noting that 27 is a cube root of 35 modulo the prime 307, find a cube root of 35 modulo 307^2.